REMARKS/ARGUMENTS

The Applicant acknowledges, with thanks, the Office Action mailed November 12, 2004. Claims 1-35 were pending, claims 1-35 stand rejected. By this amendment, independent claims 1 and 21 have been amended to recite elements and claims 2-3 and 23-24. Accordingly, claims 2-3 and 23-24 have been cancelled.

I. Rejections under 35 U.S.C. § 102

Claims 1-2, 5-6, 8, 14, 19, 21, 22, 25-27 and 37 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,243,811 to Patel (hereinafter Patel). As will be discussed further hereinbelow, independent claims 1 and 21 have been amended to add that the client reports the rogue access point to the network after authenticating with a valid access point, which is not disclosed by Patel. Claims 2, 5-6, 8, 14, 19 and 22, 25-27 and 37 depend directly from claims 1 and 21 respectively, and therefore contain each and every element of claims 1 and 21. Therefore for the reasons already set forth, claims 2, 5-6, 8, 14, 19, 22, 25-27 and 37 are not anticipated by Patel.

II. Rejections under 35 U.S.C. § 103

Independent claims 1 and 21 have been amended to incorporate elements of claims 3-4, and 23-24 respectively. Claims 3-4 and 23-24 were rejected as being obvious in view of the combination of Patel with U.S. Patent No. 6,728,782 to D'Souza et al. (hereinafter D'Souza).

Independent claim 1 as now amended, recites a method for detecting a rogue access point by a client. The method comprising the steps of directing a packet from a supplicant to a network through an access point, receiving a network response packet by the supplicant from the access point, and determining that the access point is a rogue access point based on the network response packet received from the access point in being in nonconformity with predetermined expectations. Furthermore, the method recites authenticating (the client) through a valid access point to the network and reporting the rogue access point to the network through the valid access point. Independent claim 21 recites a client configured to perform the method.

Patel, similar to the present invention, performs a mutual authentication between a mobile unit, VLR and AC/HLR). However, unlike the present invention, Patel does not report a rogue access point (or VLR) to the network after it has authenticated with a valid access point.

In rejecting claims 3 and 23 the Examiner relies on D'Souza for teaching about reporting to a network that a route has been withdrawn and in rejecting claims 4 and 24 the Examiner relies on D'Souza for teaching contacting a network by the client through a valid access point.

However, claim 1 as now amended recites authenticating (the client) through a valid access point to the network and reporting the rogue access point to the network through the valid access point. By contrast, D'Souza is directed to "a method for verifying the addition of a newly provisioned customer route as well as withdrawal of a previously provisioned route" (col. 1 lines 39-41). The present invention does not verify "provisioned routes," but improves the security of a network by verifying whether an access point purporting to belong to the network actually belongs to the network, and reporting to the network an access point that does not belong to the network through a valid access point.

D'Souza teaches that typically a customer will advertise available routes for receiving inbound data from senders of such data. If the ISP servicing the customer, or any other ISP, makes a modification to an advertised route, the advertised route can become invalid (col. 1 lines 67 - col. 2 line 8). D'Souza recites that a customer into a route provisioning system information of a new route (or withdrawal of an existing route) for advertisement to the Internet via ISP's (col. 2, lines 13-15). The Route provisioning system performs an authentication check on a new route entered by a customer that includes the following: the originating customer owns the network address, there is no conflict between the new network address and any previously provisioned network address, there exists an alternate route advertisement for the new network address, and other local policies are satisfied such as the size of the route (col. 2 lines 23-49). By contrast, the present invention does not use a 'route provisioning system' and the verification of an access point is implemented by a mobile client. Furthermore, D'Souza also teaches withdrawal of an existing route advertisement generally requires no verification (col. 2 lines 54-55). Thus, as can be seen from the foregoing, D'Souza validates routes by determining who owns a network address, checks for conflicts, and checks if a route is valid by determining if packets routed through a specified route reach their destination. However, D'Souza does not teach, suggest or show a client attempting to mutually authenticate with an access point,

determining that an access point is a rogue based on its response during authentication, nor does it teach reporting the rogue access point to the network after authenticating with a valid access point.

Thus for the reasons just set forth, neither Patel nor D'Souza when taken alone or in combination teach, suggest or show the present invention as now claimed. The aforementioned deficiencies in Patel and D'Souza are not remedied by any teaching of Zhang (US Patent Application Publication 2002/1074335) and/or Ayyargi (US Patent Application Publication No. 2002/0176366).

III. Conclusion

For the reasons set forth above, the claims of the present invention as now amended are not anticipated by the cited prior art. Furthermore, the cited prior art, taken alone or in combination, does not teach suggest or show the present invention as now claimed. If there are any fees necessitated by the foregoing communication, please charge such fees to our Deposit Account No. 50-0902, referencing our Docket No.

Respectfully submitted,
TUCKER, ELLIS & WEST

Date: 2-14-2005

Larry B. Donovan
Registration No. 47,230
1150 Huntington Building
925 Euclid Avenue
Cleveland, Ohio 44115-1475
Customer No. 23380
(216) 696-3864 (phone)
(216) 592-5009 (fax)